MICRO FOCUS

ZENworks 2020
Full Disk Encryption Agent Reference

October 2019

Legal Notice

Contents

About This Guide

The *ZENworks Full Disk Encryption Agent Reference* provides information to help you manage the Full Disk Encryption Agent. The information in this guide is organized as follows:

Audience

This guide is intended for ZENworks administrators who need to configure, manage, and troubleshoot the Full Disk Encryption Agent.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Full Disk Encryption Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks documentation website.

1 Agent Installation and Removal

In this chapter you will find the system requirements and information for installing and removing the Full Disk Encryption Agent and how to decommission a device or move a device to another management zone.

For updating the Full Disk Encryption Agent from a ZENworks 2017 (17.0) or earlier version, see the ZENworks 2020 - Full Disk Encryption Update Reference.

System Requirements

Refer to the sections in this chapter to learn about full disk encryption requirements for managed devices and pre-boot authentication.

Managed Device Requirements

The "Managed Device Requirements" in the *ZENworks 2020 System Requirements*, provides a list of software and hardware requirements that must be met to install the ZENworks Agent on a device. Devices that you want to use for ZENworks Full Disk Encryption must meet those requirements. Exceptions to those requirements are provided in the following list:

Item	Requirements
Operating System	ZENworks Full Disk Encryption is not supported on all operating systems listed in "Managed Device Requirements" in the *ZENworks 2020 System Requirements* reference. The supported operating systems for ZENworks Full Disk Encryption are: ◆ Windows 7 (x86 and x86_64) SP1 — Professional, Ultimate, and Enterprise editions only ◆ Windows 8 (x86 and x86_64) — Professional and Enterprise editions only ◆ Windows 8.1 and Windows 8.1 Update (x86 and x86_64) — Professional and Enterprise editions only ◆ Windows Embedded 8.1 Industry Pro ◆ Windows 10 (x86 and x86_64) — Professional, Education, Enterprise, and Enterprise LTSB editions
Virtual Environments	ZENworks Full Disk Encryption is not supported in all virtual environments. This includes both virtual machines and machines accessed via thin-clients. When installing the ZENworks Agent to a virtual environment machine, do not enable Full Disk Encryption on VMs configured for SCSI drives. Pre-boot authentication should also not be used on VMs configured as "Thin Clients."

Item	Requirements
Firmware	◆ Both BIOS and UEFI firmware are supported.
Disks	◆ IDE, SATA, and PATA disk interface standards are supported. SCSI and RAID hard disks are not supported. ◆ Multiple disks (one primary and multiple secondary) are supported in one device. When using multiple disks, all disks must be the same (for example, all IDE or all SATA).
Disk Communication Modes	◆ ATAPI and AHCI are supported. ◆ When using ZENworks Pre-Boot Authentication, we strongly recommend that you use the standard Microsoft drivers. Other drivers can cause issues such as CD and DVD drives disappearing.
Disk Types	◆ Basic disks are supported. Dynamic disks and other disk types are not supported.
Disk Encryption	◆ Software encryption on standard, solid state, and self-encrypted drives is supported. Encryption is not supported on devices with more than one of these types of hard drives on the same device.
File System	◆ NTFS is supported. FAT32 and all other file system formats are not supported.
System Disk	◆ The system disk (operating system) must be Disk0.
Partition Tables and Partitions	◆ Disks can use a master boot record (MBR) or GUID partition tables (GPT), both types are supported. ◆ ZENworks Full Disk Encryption creates a primary partition (referred to as the ZENworks primary partition) on the system disk to store files required for encryption and pre-boot authentication. Windows supports a maximum of four primary partitions; one primary partition must be available for ZENworks Full Disk Encryption. If all four primary partitions already exist, ZENworks Full Disk Encryption cannot create the required ZENworks primary partition and encryption fails. **Non-GPT:** A maximum of 10 partitions can be encrypted. The partitions can be on one disk or spread across multiple disks. **GPT:** A maximum of 128 partitions can be encrypted per disk.
Windows Secure Boot	◆ Secure Boot is supported for Full Disk Encryption.
Disk Space	◆ 500 MB of free disk space on the system disk (Disk0) for the ZENworks primary partition is created when the Disk Encryption policy is applied. To create the 500 MB partition, 500 MB of disk space must be available or the creation process will fail. ◆ At least 200 MB of free disk space on the system disk (Disk 0) for ZENworks Full Disk Encryption software files.

Pre-Boot Authentication Requirements

ZENworks Pre-Boot Authentication (PBA) requires the following:

Item	Requirements
Drivers	We strongly recommend that you use the Microsoft IDE/SATA drivers. Other drivers can cause issues such as CD and DVD drives disappearing.

Item	Requirements
Smart Cards	ZENworks PBA supports smart card authentication. For a list of supported smart card solutions, see Appendix A, “Supported Smart Card Terminals and Tokens,” on page 29.
Single Sign-On	ZENworks PBA supports single sign-on with Windows via both the Windows Client and the Novell Client. When using the Novell Client, the following requirements apply: ◆ Novell Client 2 SP3 IR5 or later is required on Windows 7/8/10. ◆ When using user ID/password authentication with the Novell Client and DLU, the user needs to log in to the Novell Client once before single sign-on will work. During single sign-on, the ZENworks PBA passes the user ID and password to the Novell Client. However, the client requires other details (tree, server, context, and so forth) that are available only if the user has populated the details during a previous log in. ◆ When using smart card authentication with the Novell Client, NESCM (Novell Enhanced Smart Card Method), and DLU, the user needs to be the last user to have logged in to the Novell Client. During single sign-on, the ZENworks PBA passes the pin to the Novell Client. However, the client requires other details (tree, server, context, and so forth) that are available only if the user was the last smart card user to log in to the client. ◆ Smart card authentication with the Novell Client, NESCM, and **Disconnected Workstation Only** mode is not supported.

Installing the Full Disk Encryption Agent

The Full Disk Encryption Agent is the ZENworks Agent module that is responsible for enforcing Disk Encryption policy settings on managed devices. Because it is a module, it can be installed, enabled, disabled, and uninstalled without affecting the other capabilities provided by the ZENworks Agent. The following operational states are possible for the Full Disk Encryption Agent:

- **Installed and enabled:** The Full Disk Encryption Agent is installed and can enforce a Disk Encryption policy assigned to the device.
- **Installed and disabled:** The Full Disk Encryption Agent is installed but its drivers are not loaded. Therefore it cannot enforce a Disk Encryption policy assigned to the device.
- **Uninstalled:** The Full Disk Encryption Agent is not installed on the device.

By default, the Full Disk Encryption Agent is installed and enabled on managed devices if ZENworks Full Disk Encryption is activated in either license mode or evaluation mode. If you want to change the operational state of the agent, see the instructions in “Customizing the Agent Features” in the *ZENworks Discovery, Deployment, and Retirement Reference*.

Uninstalling the Full Disk Encryption Agent

There are several methods you can use to uninstall the Full Disk Encryption Agent from a device: uninstalling it via the ZENworks Control Center, uninstalling it locally on the device, or uninstalling the ZENworks Agent.

Using ZENworks Control Center to Uninstall the Full Disk Encryption Agent

The recommended way to uninstall the Full Disk Encryption Agent is through the ZENworks Control Center:

1 If the device has a Disk Encryption policy assigned to it, remove the policy assignment in ZENworks Control Center, then refresh the device so that the policy is removed from the device.

   See "Removing Policy Assignments From Devices" in the *ZENworks Full Disk Encryption Policy Reference*.

   Removing the policy assignment causes the Full Disk Encryption Agent to decrypt the drives and remove the ZENworks PBA. Always remove the policy assignment and verify the drive is decrypted before uninstalling the agent.

2 Uninstall the Full Disk Encryption Agent:

   2a Log in to ZENworks Control Center.

   2b To uninstall the module from a single device, click **Devices**, click the device to display it's details, click the **Settings** tab, click **Device Management**, then click **ZENworks Agent**.

   or

   To uninstall the module from all device's in a device folder, click **Devices**, select the check box next to the device folder and click **Details** to display the folder details, click the **Settings** tab, click **Device Management**, then click **ZENworks Agent**.

   or

   To uninstall the module from all device's in the zone, click **Configuration**, click **Device Management** (under Management Zone Settings), then click **ZENworks Agent**.

   2c (Conditional) If you are uninstalling from a single device or a device folder, click **Override** to enable the settings to be modified.

   2d Under Agent Features, deselect the **Installed** check box for Full Disk Encryption.

   2e Click **OK** to save the change.

   2f Perform an agent refresh on the target device (or devices).

   The refresh takes longer than normal as the Full Disk Encryption Agent is removed. When the refresh completes, you can view the ZENworks Agent to verify that **Full Disk Encryption** is no longer listed in the navigation menu (select **Technician Application** in the ZENworks icon menu). In addition, the Full Disk Encryption Agent is no longer available in the **Windows Start** menu.

IMPORTANT: Deactivating the Full Disk Encryption license in ZENworks Control Center will uninstall the Full Disk Encryption Agent from all managed devices in the zone beginning when the ZENworks Agent is refreshed on each device.

Uninstalling the Full Disk Encryption Agent Locally

The recommended way to uninstall the Full Disk Encryption Agent is through the Agent Features setting in ZENworks Control Center (see Using ZENworks Control Center to Uninstall the Full Disk Encryption Agent). This method requires the device to have network access to a ZENworks Server.

If a device does not have network access, you can use the following steps to uninstall the Full Disk Encryption Agent locally:

1. Make sure you know the uninstall password for the ZENworks Agent (if one is defined).

   If an uninstall password is defined, it is required when locally uninstalling the Full Disk Encryption Agent. The password is defined in ZENworks Control Center under **Configuration** > **Management Zone Settings** > **Device Management** > **ZENworks Agent**.

2. Uninstall the Full Disk Encryption Agent:

   2a Remove the agent API by running the following Windows Installer command at a command prompt:

   For a Windows 32-bit device:

   ```
   msiexec.exe /x {1EEFEB22-7996-4F6F-82DD-89887EC9FE43} /L*v
   C:\WINDOWS\novell\zenworks\bin\zfde_api_uninstall_log.txt
   FDESHOWUNINSTALLWARNING=1
   ```

   For a Windows 64-bit device:

   ```
   msiexec /x {43A83587-0E74-4EB4-AFF6-BC040D6375F5} /L*v
   C:\WINDOWS\novell\zenworks\bin\zfde_api_uninstall_log.txt
   FDESHOWUNINSTALLWARNING=1
   ```

   2b (Conditional) If you are prompted for the uninstall password, provide the password.

   2c (Conditional) If a Disk Encryption policy is still applied to a device, you are prompted that the disk must be decrypted before the uninstall can be performed. Click **OK** to start decryption of the disk and removal of the ZENworks PBA.

   The process decrypts the disk, removes the ZENworks PBA, and reboots the device (according to the reboot option set for the policy). You can use the Full Disk Encryption Agent's About box to verify that the policy is no longer being enforced. When the process is complete, run the command in Step 2a again.

   You can view the `zfde_api_uninstall_log.txt` file to verify that the uninstall is successful. The status is recorded in the last few lines of the log file.

   2d Remove the agent drivers by running the following Windows Installer command at a command prompt (for both Windows 32-bit and 64-bit devices):

   ```
   msiexec /x {BC75322F-F526-4E22-8A0F-8CCFA046B65B} /L*v
   C:\WINDOWS\novell\zenworks\bin\zfde_sec_uninstall_log.txt
   ```

   You can view the `zfde_sec_uninstall_log.txt` file to verify that the uninstall is successful. The status is recorded in the last few lines of the log file.

   2e Remove the agent policy handler by running the following Windows Installer command at a command prompt (for both Windows 32-bit and 64-bit devices):

   ```
   msiexec /x {14588647-0376-45A8-8F81-59D2AA7B758B} /L*v
   C:\WINDOWS\novell\zenworks\bin\zfde_pol_uninstall_log.txt
   ```

   You can view the `zfde_pol_uninstall_log.txt` file to verify that the uninstall is successful. The status is recorded in the last few lines of the log file.

3. Restart the device.

To view the ZENworks Agent, select **Technician Application** in the ZENworks icon menu, and verify that **Full Disk Encryption** is no longer listed. In addition, the Full Disk Encryption Agent is no longer available in the **Windows Start** menu.

4 (Conditional) If the device will connect to a ZENworks Server in the future, disable the device's Full Disk Encryption setting in ZENworks Control Center. If the setting is enabled, the next time the device connects, the Full Disk Encryption Agent is reinstalled.

4a In ZENworks Control Center, click **Devices**, click the device to display its details, click the **Settings** tab, click **Device Management**, then click **ZENworks Agent**.

4b Click **Override** to enable the settings to be modified.

4c Under Agent Features, deselect the **Installed** check box for Full Disk Encryption.

4d Click **OK** to save the change.

Uninstalling the ZENworks Agent

You can uninstall the ZENworks Agent to remove the Full Disk Encryption Agent. This, of course, removes all other ZENworks functionality from the device.

1 If the device has a Disk Encryption policy assigned to it, remove the policy assignment in ZENworks Control Center, then refresh the device so that the policy is removed. See "Removing Policy Assignments From Devices" in the *ZENworks Full Disk Encryption Policy Reference*.

Removing the policy assignment causes the Full Disk Encryption Agent to decrypt the drives and remove the ZENworks PBA. Always remove the Disk Encryption policy assignment and verify the drive is decrypted before uninstalling the agent.

2 Make sure you know the uninstall password for the ZENworks Agent (if one is defined).

If an uninstall password is defined, it is required when locally uninstalling the ZENworks Agent or any modules such as the Full Disk Encryption Agent. The password is defined in ZENworks Control Center under **Configuration** > **Management Zone Settings** > **Device Management** > **ZENworks Agent**.

3 Uninstall the ZENworks Agent:

3a Start the uninstall through the Windows Control Panel (for example, **Uninstall a program** in Windows 7/8/10).

3b At the Welcome screen, click **Next**.

3c To uninstall the agent and unregister the device from the ZENworks Management Zone, provide the user name and password of a ZENworks administrator, click **Next**, select **Uninstall the ZENworks Agent and unregister the device from the zone,** then click **Next**.

or

To uninstall the agent only, select **Local uninstallation only (Retain the device in the zone)**, then click **Next**.

3d (Conditional) If you are prompted for the uninstall password, provide the password.

3e (Conditional) If a Disk Encryption policy is still applied to a device, you are prompted that the disk must be decrypted before the uninstall can be performed. Click **OK** to start decryption of the disk and removal of the ZENworks PBA. When the process is finished, start the uninstall again (Step 3a).

4 Restart the device.

Decommissioning a Device

You can prevent access to encrypted data by either temporarily or permanently decommissioning a device. Temporarily decommissioning a device removes all Pre-Boot Authentication (PBA) user accounts from the device; the device can be recovered through a PBA override or through the use of an emergency recovery disk. Permanently decommissioning a device erases all data on the encrypted devices; the erased data is unrecoverable.

Temporarily Decommissioning a Device

You can prevent access to encrypted data by temporarily decommissioning the device. When a device is temporarily decommissioned, all of the Pre-Boot Authentication (PBA) user accounts are removed. The only way to access the device after the users are removed is to perform a PBA override or an emergency recovery. Before decommissioning the device, you should ensure that an Emergency Recovery Information (ERI) file exists for the device (see Creating an Emergency Recovery Information File).

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To temporarily decommission a device by removing all PBA users, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 31.
2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click the **Commands** button.
4. Supply the password, then click **OK** to display the Commands dialog box.
5. Click the **Temporary Decommission** button.
6. In the confirmation dialog box that is displayed, click **Yes** to proceed.

   The device immediately shuts down.

Permanently Decommissioning a Device

You can prevent access to encrypted data by permanently decommissioning the device. You do this by erasing all of the encrypted data. The erased data is unrecoverable.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To permanently decommission a device, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 31.
2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click the **Commands** button.
4. Supply the password, then click **OK** to display the Commands dialog box.
5. Click the **Permanent Decommission** button.
6. In the confirmation dialog box that is displayed, click **Yes** to proceed.

   The device immediately shuts down.

Moving a Managed Device From One Zone to Another Zone

You can move a device to a zone where Full Disk Encryption is not active or to a zone where Full Disk Encryption is active.

Moving a Device to a Zone Where Full Disk Encryption Is Not Active

When you unregister a device from its zone, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.

If you the register the device in a zone where Full Disk Encryption is not active (or the Full Disk Encryption Agent is disabled or not installed), the Disk Encryption policy and the Full Disk Encryption Agent are removed from the device. Encrypted volumes are decrypted and the ZENworks PBA is removed.

To move a device:

1. Unregister the device. See "Unregistering a Device" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

   After the device is unregistered, the Full Disk Encryption agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.
2. Register the device in the new zone. See "Manually Registering a Device" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

   After the device registers in the zone, the Disk Encryption policy is removed and the Full Disk Encryption Agent decrypts any encrypted volumes. The ZENworks Agent then uninstalls or disables the Full Disk Encryption Agent.

Moving a Device to a Zone Where Full Disk Encryption Is Active

When you unregister a device from its zone, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.

If you then register the device in another zone (or reregister it in the same zone) and assign a Disk Encryption policy to the device, the Full Disk Encryption Agent enforces the new policy. If the new policy uses the same encryption settings (algorithm, key length, and so forth) as the device's current policy, no encryption changes take place. If the new policy has different encryption settings, any encrypted volumes are decrypted and then re-encrypted using the new encryption settings.

To move a device:

1. Unregister the device. See "Unregistering a Device" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

   After the device is unregistered, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.

2 Register the device in the new zone. See “Manually Registering a Device” in the *ZENworks Discovery, Deployment, and Retirement Reference*.

   After the device registers in the zone, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. However, because the policy is not assigned to the device through the zone, you cannot modify the policy in ZENworks Control Center.

3 (Optional) Assign a new Disk Encryption policy to the device.

   If you want to manage the Disk Encryption policy for the device, you need to assign a new policy that exists in the zone. To ensure that the device’s volumes are not decrypted and then encrypted again, make sure the new policy uses the same encryption settings (algorithm, key length, and so forth) as the device’s current policy.

2 Disk Encryption

You can view the Disk Encryption settings and decrypt drives using the ZENworks Full Disk Encryption Agent on managed devices.

Accessing the Full Disk Encryption Agent

To access the Full Disk Encryption Agent on a manage device:

1. On the device, right-click the ZENworks icon in the notification area, and select **Technician Application**.
2. Click **Full Disk Encryption** in the ZENworks Agent navigation menu.
3. In the **Full Disk Encryption Agent Actions** section, click **About** to display the Full Disk Encryption About dialog box.

Viewing the Disk Encryption Settings

The Full Disk Encryption Agent lets you view the disk encryption settings for the policy being applied to the device.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To view the disk encryption settings, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 31.
2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click **View Policy**, type the FDE Admin password for the policy, then click **OK**.

   The View Policy dialog box includes a tab for the policy’s Full Disk Encryption settings and Pre-Boot Authentication settings.
4. After you finish viewing the policy settings, click **Close** to exit the dialog box.

Decrypting Drives

You can use the Full Disk Encryption Agent to decrypt any of the device’s encrypted drives. The drive remains decrypted unless a new Disk Encryption policy is applied that causes the drive to be encrypted again.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

To decrypt a drive, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 31.

2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click the **Commands** button.
4. Supply the password, then click **OK** to display the Commands dialog box.
5. Click the **Decrypt Drive** button.
6. Select the drive to decrypt, then click **OK**.
7. In the confirmation dialog box that is displayed, click **Yes** to proceed.

WARNING: When decrypting a drive, ensure that the decryption process is not interrupted prematurely with a power change on the device; otherwise, all data on the disk can be lost due to disk corruption. You can check the decryption status on the device by accessing **Full Disk Encryption** > **About** in the ZENworks Agent.

Disk corruption due to power change has only been noted on secondary drives, but it may also be applicable to primary drives. For this reason, the following precautions are strongly recommended before decrypting a device drive:

- Pre-configure device drives that will be decrypted so that power options are set to never automatically shut off, hibernate, or sleep.
- Inform all device users of the need to keep the device(s) running during the decryption process, to include avoiding Sleep and Hibernation options.

  This precaution is for user actions that are not a part of the reboot process that is required for decryption.

---

3 Pre-Boot Authentication

Refer to sections in this chapter to learn about viewing PBA settings, enabling User Capturing, managing PBA user accounts, and synchronizing the PBA and Windows credentials.

Viewing the Pre-Boot Authentication Settings

The Full Disk Encryption Agent lets you view the pre-boot authentication settings for the policy being applied to the device.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To view the pre-boot authentication settings, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, "Administrator Passwords," on page 31.
2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click **View Policy**, type the FDE Admin password for the policy, then click **OK**.

   The View Policy dialog box includes a tab for the policy's pre-boot authentication settings.
4. After you finish viewing the policy settings, click **Close** to exit the dialog box.

Enabling User Capturing

You can use the Full Disk Encryption Agent to enable user capturing for pre-boot authentication. Enabling user capturing causes ZENworks Pre-Boot Authentication to capture the credentials (user ID/password or smart card) of the first user to log in after the device is rebooted.

You can also use ZENworks Control Center to enable user capturing on a device. For information, see "Enabling User Capturing" in the *ZENworks Full Disk Encryption PBA Reference*.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To enable user capturing, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, "Administrator Passwords," on page 31.
2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click the **Commands** button.

4 Supply the password, then click **OK** to display the Commands dialog box.

5 Click the **Enable User Capture** button.

You can verify the setting by viewing the agent status and looking at the **PBA Self Initialization Mode** value (see Viewing the Agent Status). If user capturing is enabled, the value will be `WINDOWS_CRED_SELFINIT`.

Managing PBA User Accounts

You can use the Full Disk Encryption Agent to add or delete user accounts for ZENworks Pre-Boot Authentication (PBA). PBA user accounts you add exist only on the device; they are not added to the Disk Encryption policy. In addition, if the **Remove existing users from PBA if not in this list** option is enabled in the Disk Encryption policy, the added user is removed after the next login.

You can also use ZENworks Control Center to add PBA users on a device. For information, see "Manually Adding Users" in the *ZENworks Full Disk Encryption PBA Reference*.

1 Make sure you know the FDE Admin password for the policy that is assigned to the device.

To add or remove a PBA user account, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, "Administrator Passwords," on page 31.

2 Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.

3 Click the **Commands** button.

4 Supply the password, then click **OK** to display the Commands dialog box.

5 Click the **Add/Delete PBA User** button.

6 Provide the username, password, and domain of the user you want to add or delete.

If the user is not part of a Windows domain, specify the computer name instead.

7 (Conditional) If you want to delete the user, select the **Check to Delete User** box.

8 Click **OK** to add or delete the user.

You can verify the change by viewing the agent status and looking at the **PBA User List** (see Viewing the Agent Status).

Synchronizing the PBA and Windows Credentials

This information applies only if ZENworks Pre-Boot Authentication (PBA) is installed on the device.

If a device's Disk Encryption policy has single sign-on enabled so that the ZENworks PBA login credentials are the same as the Windows login credentials, the passwords remain synchronized if the Windows password is changed through one of the following methods:

- Via Windows domain login
- Via Windows local login
- Using Ctrl+Alt+Del to access the change password feature

The passwords are not synchronized if one of the following methods is used:

- Control Panel
- Device Manager

If the passwords become out-of-sync, the following methods can be used to synchronize them while at the device:

- “Using the Windows Login” on page 21
- “Using the Full Disk Encryption Agent” on page 21

In addition, you can use a ZENworks Control Center Quick Task to synchronize the passwords. For information, see “Synchronizing PBA and Windows Credentials” in the *ZENworks Full Disk Encryption PBA Reference*.

Using the Windows Login

This is the recommended way to synchronize a user’s PBA and Windows passwords because the user can complete these steps without administrator assistance:

1. Restart the device.
2. Log in to the ZENworks PBA using the old Windows/PBA password.
3. When the Windows login screen is displayed, enter the password required to log in to Windows.

   The ZENworks PBA detects the difference in the current PBA and Windows passwords and changes the PBA password to the Windows password.
4. Restart the device and log in to the ZENworks PBA using the new Window/PBA password.

Using the Full Disk Encryption Agent

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To change the user’s PBA password, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 31.
2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click the **Commands** button.
4. Supply the password, then click **OK** to display the Commands dialog box.
5. Click the **Add/Delete PBA User** button.
6. Provide the following:

   User Name: Specify the user name for the user whose password you want to change.

   User Password: Specify the user’s Windows password. This becomes the PBA password.

   User Domain: Specify the user’s Windows domain name. If the user is not a member of a domain, you can specify the computer name or leave the field blank.

   If you don’t know the domain or computer name, you can cancel to exit the dialog box, close the ZFDE Commands dialog box, click the **Agent Status** button, click the **PBA** tab, then scroll down to the **User List** at the bottom of the page. The user name and domain/computer name are listed in the **PBA User Name** column, with the domain/computer name listed second (after the colon).
7. Click **OK** to change the PBA password.

4 Troubleshooting

There are several resources available to troubleshoot Full Disk Encryption issues, including Agent Status, log files, and diagnostics packages.

Viewing the Agent Status

The Full Disk Encryption Agent provides a variety of status information related to the enforcement of the Full Disk Encryption policy on the device. For example, the agent displays the current enforcement settings for both encryption and pre-boot authentication. It also lists the Emergency Recovery Information (ERI) files created for the device and shows the enforcement history for previous Full Disk Encryption policies or versions applied to the device.

To view the Full Disk Encryption Agent status information:

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To view the agent status, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 31.
2. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
3. Click **Agent Status**, in the Full Disk Encryption dialog box, type the FDE Admin password for the policy, and then click **OK**.

   The Agent Status dialog box includes tabs for Full Disk Encryption status, Pre-Boot Authentication (PBA) status, and general agent settings status.
4. After you finish viewing the status pages, click **Close** to exit the dialog box.

Creating an Emergency Recovery Information File

If a situation occurs where a user cannot access the encrypted volumes on a device, you might need to perform an emergency recovery of the device. This requires an Emergency Recovery Information (ERI) file for the device.

An ERI file is a password-protected file that contains the encryption keys for the encrypted volumes of the device’s hard disk. The file is the only way to get in to the device in an emergency.

By default, whenever the ZENworks Full Disk Encryption Agent changes the encryption settings (volumes, algorithm, and so forth) for the hard disk, an ERI file is created and sent to the ZENworks server to be stored on your network.

If a user infrequently connects to the network, or if you simply want to ensure that the user has a personal backup copy of the ERI file, you or the user can manually create an ERI file and store it in a secure location other than the device's local hard disk. For example, a removable storage device such as a USB drive could be used.

To create an ERI file:

1. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
2. Click the **Create ERI File** button if it is available.

   or

   If the **Create ERI File button** is not available, click **Commands**, specify the password to display the Commands dialog box, then click the **Create ERI** button.

   The **Create ERI File** button is only available in the About dialog box if the feature has been enabled in the Disk Encryption policy applied to the device. However, the Create ERI button is always available in the Commands dialog box. To access the Commands dialog box, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Agent override password or key. For more information about passwords, see Appendix B, "Administrator Passwords," on page 31.
3. When you are prompted to assign a password to the ERI file that will be generated, specify a password, then click **OK**.

   If a strong password is required, it must include at least one uppercase letter, one lowercase letter, one number, and one special character. Special characters are:

   ~ ! @ # $ % ^ & * ( ) _ + { } [ ] : ; < > ? , . / \ - = | "

   Make sure the password is one that you can remember. The password is required to use the ERI file for an emergency recovery.

   The Full Disk Encryption Agent creates a *computer-name_yyyy_mmdd_hhmm*.eri file on your desktop (for example, computer1_2011_1208_1435). If you are connected to the ZENworks server on your network, it is also sent to the server.
4. Copy the ERI file to a secure location that is still accessible when the device is not.

Logging Agent Events

The Full Disk Encryption Agent logs information to the device's local disk. The log files can be used in conjunction with Micro Focus Support to troubleshoot issues with Full Disk Encryption.

Log Files

The ZENworks Full Disk Encryption Agent consists of multiple processes and drivers, each of which performs specific functions related to policy handling and disk encryption. Four of these processes log activities to their own files:

- **Log_*YYYYMMDD_HHMMSS_NNNN*.txt:** This log contains any Full Disk Encryption messages generated by the ZESService.exe process. This agent process performs the majority of activities for Full Disk Encryption.
- **Cmd_*YYYYMMDD_HHMMSS_NNNN*.txt:** This log contains any Full Disk Encryption messages generated by the ZESCommand.exe process. This agent process executes agent commands (such as creating diagnostic packages) from a command line.

- **User_*YYYYMMDD_HHMMSS_NNNN*.txt:** This log contains any Full Disk Encryption messages generated by the `ZESUser.exe` process. This agent process executes agent commands (such as creating diagnostic packages) through the user interface.
- **ZID_*YYYYMMDD_HHMMSS_NNNN*.txt:** This log contains any Full Disk Encryption messages generated by the `ZESZid.dll` process. This agent process communicates policy data between the ZENworks Agent and the `ZESService.exe` process.

The log files are stored in the following hidden directory:

Windows 7/8/10: `c:\ProgramData\Novell\ZES\Logs`

Each process creates a new log file when the process starts or when the log file reaches approximately 1 MB. A maximum of 10 log files are kept for `ZESService.exe`, `ZESCommand.exe`, and `ZESZid.dll`, and a maximum of 50 log files are kept for `ZESUser.exe`.

The Full Disk Encryption Agent drivers also generate two log files: `FDE.log` and `PBA.log`. These logs are stored in the same directory as the process logs. These are low-level logs that provide information for Micro Focus Support if needed.

Accessing the Logging Settings

The `ZESService.exe`, `ZESCommand.exe`, `ZESUser.exe`, and `ZESZid.dll` processes are shared processes used by the ZENworks Full Disk Encryption Agent, the ZENworks Endpoint Security Agent, and the ZENworks Location Decider. Because of this, the logging settings are accessed through the ZENworks Endpoint Security Agent if it is enabled, or through the ZENworks Location Decider if the Endpoint Security Agent is not enabled.

1. On the device, right-click the ZENworks icon in the notification area, and select **Technician Application**.
2. Click **Agent** under the **Status** heading in the ZENworks Agent navigation menu.
3. In the **Agent Security Settings** section, click **Security Settings Details**.

   If ZENworks Endpoint Security Management is enabled, the ZENworks Endpoint Security Agent dialog box is displayed. If it is not enabled, the ZENworks Location Decider dialog box is displayed.
4. Click the **Diagnostics** button.
5. Click **Logging**.

Changing the Logging Level

By default, the logging level is set to Warning. If necessary, you can change it to Debug, Informational, or Error to gather more or less information. For troubleshooting, you should set logging according to the directions of ZENworks Support and re-create the circumstances that led to the error to see if it can be repeated.

To change the logging level:

1. Access the Logging dialog box. If you need instructions, see Accessing the Logging Settings.
2. Change the **Full Disk Encryption** logging level as desired:

   Debug: Turns on every possible message and includes Informational, Warning, and Error messages.

   Informational: Records all events when they occur, such as when a network connection event begins and ends.

Warning: Records errors that have occurred but are solvable and do not prevent the client from running.

Error: Records errors that have occurred and prevent the client from running.

3 If you want to save the settings as the default settings, select **Save as Defaults**. Otherwise, the settings are used only for the current session for each process (`ZESCommand.exe`, `ZESService.exe`, and `ZESUser.exe`).

If you change settings, you can click **Restore Defaults** to reset them to the stored defaults.

4 Click **OK** to exit the dialog box.

Viewing Log Files

1 Access the Logging dialog box. If you need instructions, see Accessing the Logging Settings.

2 Click one of the following buttons to display the log file you want:

- **View Service Log:** This log contains any Full Disk Encryption messages generated by the `ZESService.exe` process. This agent process performs the majority of activaties for Full Disk Encryption.
- **View User Log:** This log contains any Full Disk Encryption messages generated by the `ZESUser.exe` process. This agent process executes agent commands (such as creating diagnostic packages) through the user interface.
- **View Interface Log** This log contains any Full Disk Encryption messages generated by the `ZESZid.exe` process. This agent process communicates policy data between the ZENworks Agent and the `ZESService.exe` process.

3 When you are finished viewing log files, click **OK** to exit the dialog box.

Inserting a Comment in the Log Files

You can add your own comment to the Service (`Log_*.txt`) and User (`User_*.txt`) logs. The comment is inserted at the current line in both of the log files.

1 Access the **Logging** dialog box. If you need instructions, see Accessing the Logging Settings.

2 Click **Add Comment** to display the Comment dialog box.

3 Type your comment, then click **OK** to add it to the log files.

4 View the log files, or click **OK** to exit the Logging dialog box.

Deleting All Log Files

You can delete all log files from a managed device. The current log files and any saved log files are deleted.

1 Access the Logging dialog box. If you need instructions, see Accessing the Logging Settings.

2 Click **Clear Log Files**.

3 Click **OK** to exit the dialog box.

Creating a Diagnostics Package

If Micro Focus Support is helping you resolve a Full Disk Encryption Agent issue on one of your devices, you might be asked to generate a diagnostic package for Support to review. This package contains information about the device's Group Policy object, registry settings, system, and system events.

To create a diagnostics package:

1. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
2. Click **Diagnostics**, and follow the prompts to create the package.

   The Full Disk Encryption Agent creates an `fdediagnostics*.enc` file on your desktop. This can take a while. During the creation time, the Diagnostics button is disabled.

   After the file is created, send it to Micro Focus Support.

Viewing the List of Agent Modules

You can view a list of the Full Disk Encryption Agent modules that are currently loaded on a device. The list displays each module with its date and version.

1. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
2. Click **Module List**.
3. After you finish viewing the module list, click **Close** to exit the dialog box.

Bypassing PBA for Specified Reboots

If you need to temporarily bypass pre-boot authentication on a device for application installations or for any other reason, you can configure the device to skip PBA for a designated number of reboots.

To bypass PBA for specified reboots:

1. Open the Full Disk Encryption agent on the managed device. See Accessing the Full Disk Encryption Agent.
2. Click **Commands**.
3. Enter the FDE Admin password and click **OK** to display the Commands dialog box.
4. Select the number of reboots you want to bypass in the drop-down box next to the **Bypass PBA for Specified Reboots** button.
5. Click **Bypass PBA for Specified Reboots**.

NOTE: This action can also be performed from the Command Prompt. For instructions, see Bypassing PBA for Reboots using the Command Line.

Overriding Bypass of PBA for Specified Reboots

To override a PBA bypass command that has already been executed but still has one or more reboots remaining in the count, follow the procedure in Bypassing PBA for Specified Reboots, and use **0** as the number of desired reboots to bypass.

Bypassing PBA for Reboots using the Command Line

To bypass PBA for a specified number of reboots using the command line:

1. Open the Command Prompt and change the directory to `%ZENWORKS_HOME%/esm/`.

   For example: `cd %ZENWORKS_HOME%/esm/`

2. Enter the following command: `zescommand bypassPbaWithRebootCount <RebootCount> <PasswordKey>`

   For example: `zescommand bypassPbaWithRebootCount 3 01mYPwd053`

   Enter one of the following for the Password Key:

   - Password key (generated by the administrator)
   - ZENworks Agent override password
   - FDE Admin password

NOTE: To override a PBA bypass command that has already been executed but still has one or more reboots remaining in the count, follow the same procedure as above using **0** as the reboot count.

A Supported Smart Card Terminals and Tokens

Beginning in ZENworks 2017 Update 1, pre-boot authentication uses an upgraded CCID device manager, so the Smart Card Reader setting is permanently configured to **AUTO Detect** devices for the reader type. This enhancement makes incompatibility uncommon with UEFI devices.

After upgrading Full Disk Encryption to a 2017 Update 1 or later version, legacy BIOS devices will not support the following smart card terminals:

- Kobil B1 PCMCIA
- Kobil B1 Professional
- Kobil B1S Professional
- O2 Micro
- O2 Micro PCMCIA
- RicohPCI
- SCM SCR 241/243

NOTE: For supported smart card terminals and tokens pre-ZENworks 2017 Update 1, see the ZENworks 2017 documentation.

Integrated PKCS#11 Middleware. The following PKCS#11 middleware is integrated into the Linux-based Pre-Boot Authentication component:

- A.E.T. SafeSign PKCS#11
- Aladdin PKCS#11
- Charismathics
- Cryptovision
- Gemalto .NET
- KOBIL PKCS#11
- Oberthur
- RSA SecurID 800 PKCS#11
- Schlumberger
- SECUDE PKCS#11
- SECUDE TCOS
- TCrypt 11

NOTE: a.Trust PKCS providers are not supported for UEFI devices.

B Administrator Passwords

The Full Disk Encryption Agent provides several features that are intended for use only by a ZENworks administrator or by a user under the direction of a ZENworks administrator. These features are grouped together in the Full Disk Encryption Agent's About dialog box.

In order to use the Administrator features, you must provide the FDE Admin password for the Full Disk Encryption policy assigned to the device, or you must have enabled a ZENworks Agent override password. If you use an override password on a device, we recommend the following practice:

- If you are the one using the override password on a device, you can use the password as defined in the ZENworks Agent Security settings in ZENworks Control Center.
- If you are allowing a user to access the Administrator options, you should generate an override password key for the user. The key functions like the override password but allows you to specify who can use the key, what device it can be used on, and when the key expires. Using a key enables you to maintain the security of your override password and impose override restrictions on the key. For information about generating an override password key, see "Password Key Generator" in the *ZENworks Endpoint Security Utilities Reference*.